Follow us On Twitter

DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

August 2013 Issue


# DTI eSecurity News — Email Phishing Attacks


Email is one of the primary ways we communicate, whether at work or to stay in touch with friends and family. Companies use email to provide many products or services, such as confirmation of an online purchase or electronic bank statements. Since so many people depend on email, phishing has become one of the preferred attack methods used by cyber criminals.

## How Do You Protect Yourself?

- Be suspicious of any email that requires "immediate action".
- Be suspicious of emails addressed to "Dear Customer" or other generic salutation.
- Be suspicious of grammar or spelling mistakes.
- Do not click on links. Instead, copy the URL from the email and paste it into your browser ,or type the destination name into your browser.
- Hover your mouse over the link. This will show you the true destination of where you will go if you click on the link. If the 'true' destination of the link is different than that shown in the email, this may be an indication of a fraud attempt.
- Be suspicious of attachments, and only open those that you are expecting.


## How Do Phishing Attacks Work?

Phishing is a social engineering technique where cyber attackers attempt to fool you into taking an action. Often, these attacks begin when a cyber criminal sends an email, pretending to be someone or something you trust. These emails are crafted to look convincing enough to entice you to take an action, such as clicking on a link, opening an attachment, or responding to the email message.

- **Harvesting Information:** The attacker's goal is to fool you into clicking on a link that takes you to a website that looks legitimate and asks for your login and password or perhaps your credit card or ATM number.
- **Infecting your computer with malicious links:** The attacker's goal is for you to click on a link. If you click on the link, you are directed to a website that silently launches an attack against your computer. If the attack is successful, it will infect your system.
- **Scams:** These are attempts by criminals to defraud you. Examples are notices that you have won the lottery or charities requesting donations after a disaster. Don't be fooled, these are scams by criminals who are after your money.

*Produced in part from SANS*

**How good are you at spotting phishing emails?**

*Brush up on your skills. by taking a Phishing IQ test.*

**Questions or comments?**

E-mail us at eSecurity@state.de.us